山东理工大学校长办公室文件

鲁理工大办发〔2019〕11 号

校长办公室关于印发《山东理工大学网络与信息安全应急预案》的通　知

各学院、研究院，校行政各部门、各直属单位，经济与管理学部：

《山东理工大学网络与信息安全应急预案》业经研究同意，现予以印发，请结合实际，认真贯彻执行。

校长办公室

2019 年 7 月 1 日

山东理工大学网络与信息安全应急预案

1 总则

1.1 编制目的

为建立健全学校网络与信息安全应急工作机制，提高应对网络与信息安全突发事件的能力，预防和减少网络与信息安全突发事件的危害，维护学校安全稳定，特制定本预案。

1.2 编制依据

《中华人民共和国网络安全法》《国家网络安全事件应急预案》（中网办发文〔2017〕4号）《信息安全事件分类分级指南》（GB/Z 20986-2007）《教育系统网络安全事件应急预案》（教技〔2018〕8号）等相关规定。

1.3 适用范围

本预案适用于学校网络与信息安全突发事件，指导全校网络与信息安全突发事件的应对处置工作。

1.4 工作原则

统一指挥，密切协同。学校网络安全与信息化工作领导小组统筹协调学校网络与信息安全应急指挥工作，建立与国家网络安全职能部门、专业机构等多方参与的协调联动机制，做到快速响应、正确应对、果断处置。

明确责任，加强协作。依照“统一领导，快速反应，密切配合，科学处置”的组织原则和“谁主管谁负责、谁运行谁负责、谁使用谁负责”的协调原则，各司其职，各尽其力，认真履行应

急处置工作的管理职责。各部门、各单位党政主要负责人是网络安全工作第一责任人。

预防为主，防治结合。立足安全防护，加强预警，采取多种措施，共同构筑网络与信息安全保障体系。提高网络与信息安全事件快速响应和科学处置的能力，抓早抓小，严控网络安全事件的风险和影响范围。

2 事件分类分级

2.1 事件分类

网络与信息安全事件分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他事件等。

有害程序事件分为计算机病毒事件、蠕虫事件、特洛伊木马事件、僵尸网络事件、混合程序攻击事件、网页内嵌恶意代码事件和其他有害程序事件等。

网络攻击事件分为拒绝服务攻击事件、后门攻击事件、漏洞攻击事件、网络扫描窃听事件、网络钓鱼事件、干扰事件和其他网络攻击事件。

信息破坏事件分为信息篡改事件、信息假冒事件、信息泄露事件、信息窃取事件、信息丢失事件和其他信息破坏事件。

信息内容安全事件是指通过网络传播法律法规禁止信息，组织非法串联、煽动集会游行或炒作敏感问题并危害国家安全、社会稳定和公众利益的事件。

设备设施故障分为软硬件自身故障、外围保障设施故障、人为破坏事故和其他设备设施故障。

灾害性事件是指由自然灾害等其他突发事件导致的网络与信息安全事件。

其他事件是指不能归为以上6个基本分类的安全事件。

2.2 事件分级

网络与信息安全事件分为四级：特别重大(Ⅰ级)、重大（II级）、较大（III级）、一般（Ⅳ级）。

特别重大（Ⅰ级）

网络与信息系统发生全局性大规模瘫痪，事态发展超出学校的控制能力，对国家安全、社会秩序、学校利益造成特别严重损害的突发事件。

学校的重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对学校安全和稳定构成特别严重威胁。

重大（II级）

网络与信息系统造成全局性瘫痪，对国家安全、社会秩序、学校利益造成严重损害，需要上级相关部门协同处置的突发事件。

学校的重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对学校安全和稳定构成严重威胁。

较大（III级）

某一部分的网络与信息系统瘫痪，对学校的网络安全、教育教学秩序、教师和学生的权益造成一定损害，但可以在一定时间内通过相应技术手段进行重建和恢复，不需要跨部门协同处置的突发事件。

学校的重要敏感信息和关键数据丢失或被窃取、篡改、假冒，对学校安全和稳定构成较严重威胁。

一般（Ⅳ级）

单一网络与信息系统受到一定程度的损坏，对教师和学生的教育教学、办公及宣传工作有一定影响，但不危害学校的网络整体安全和秩序的突发事件。

3 应急处置机构与职责

3.1 应急处置机构

全校网络与信息安全事件应急处置工作由学校网络安全与信息化工作领导小组统一指挥、指导、协调；必要时成立安全事件应急指挥部。各相关部门、单位必须坚决执行领导小组的决定，密切配合，履行职责。

3.2 相关职责

组织机构	职责
网络安全与信息化工作领导小组	决定Ⅰ级和Ⅱ级网络与信息安全事件应急预案的启动。 统筹协调国家和学校重要节日、重大活动和会议期间网络安全保障工作，加强网络安全监测和分析研判，预警可能造成重大影响的风险和隐患，及时发现和处置网络安全事件隐患。 督促检查安全事件处置情况及各有关部门、单位在安全事件处置工作中履行职责情况。 对全校各部门、各单位贯彻执行应急处置预案、应急处置准备情况进行督促检查。
党委(校长)办公室、保密办公室	组织协调有关部门、单位查处利用计算机网络泄密的违法行为。 牵头组织重大敏感时期、重要活动、重要会议期间发生的信息安全事件的协调处置。
党委宣传部	负责学校舆情监测，对于涉及师生政治思想方面的倾向性、苗头性问题加强分析研判。 负责舆情突发事件的处置。 负责应急处置过程中的舆论处置。
安全管理处	密切配合公安部门，做好网络与信息安全事件的处置工作。 负责及时收集、通报和上报网络与信息安全事件应急处置情况。
网络信息中心	负责校园基础网络系统安全。 负责计算机病毒疫情和大规模网络攻击事件的处置。 负责校级网络与信息系统安全事件处置的技术支持。

其他单位	负责本单位内部的网络与信息安全管理和突发事件应急处置，对照本预案建立单位内部应急处置机制。 配合各部门、单位落实相关应急处置措施。

4 网络与信息安全事件应急响应机制

4.1 I 级应急响应：网络信息中心与相关部门、单位先行通过技术手段紧急处置，同时将具体情况上报学校网络安全与信息化工作领导小组和分管校领导。学校网络安全与信息化工作领导小组会商后将事件详细情况上报省教育厅、省委教育工委和公安机关等政府相关应急指挥机构，由上级部门会同学校统一协调指挥后续应急处置工作。

4.2 II 级应急响应：网络信息中心与相关部门、单位先行通过技术手段紧急处置，同时将具体情况上报学校网络安全与信息化工作领导小组和分管校领导，由学校网络安全与信息化工作领导小组统一协调指挥网络信息中心、党委（校长）办公室、党委宣传部、安全管理处等相关职能部门开展后续应急处置工作。

4.3 III 级应急响应：网络信息中心和相关业务部门协同开展应急处置工作，有关情况备案后报分管校领导。

4.4 IV 级应急响应：网络信息中心负责应急处置工作，处置结果通报相关业务部门。

5 应急技术处理程序

基于网络与信息安全事件的不同形式，针对性的实施以下应急技术处理程序：

5.1 灾害性事件：判断灾害发生实际情况，在人身安全有保障的前提下，重点保障数据安全，及时迁移灾害现场的数据硬盘。灾害性事件视情况采取 I 或 II 级响应。

5.2 设备故障事件：迅速定位设备故障地点和故障原因，调取备用设备或模块立即替换，优先保证校园网主干网络和重要信息系统、业务系统的运转。设备故障事件视情况采取 I 至 IV 级响应。

5.3 信息内容安全事件：发生学校信息发布系统违规发布信息时，相应业务主管部门应迅速报告网络信息中心屏蔽该系统的网络端口或拔掉网络连接线，阻止有害信息的进一步传播。网络信息中心根据相关日志记录查找信息发布人，及时定位信息源，会同相关部门单位做好善后处理工作。对于公安机关要求学校协助调查由校内发出的外网不良信息事件，根据网络安全设备相关记录查找信息发布人。信息内容安全事件视情况采取 I、II 或 III 级响应。

5.4 信息破坏事件：发生学校信息系统数据被非法篡改（或数据丢失）、信息泄露等重大事件时，相应业务主管部门应迅速报告网络信息中心屏蔽该系统的网络端口或拔掉网络连接线，阻止有害信息的进一步传播。网络信息中心根据相关日志记录查找信息发布人，及时定位攻击源，会同相关部门单位做好善后处理工作。对于公安机关要求学校协助调查由校内发出的外网不良信息事件，根据网络安全设备相关记录查找攻击源。信息内容安全事件视情况采取 I、II 或 III 级响应。

5.5 网络攻击事件：调取防火墙、行为审计系统等相关网络安全设备数据，判断攻击的来源与性质，关闭影响安全与稳定的网络设备和服务器设备。涉及网络核心设备、重要信息发布服务器或信息系统服务器受到攻击，可先断开设备与攻击源的网络物

理连接，跟踪并锁定攻击来源的 IP 地址或其他网络用户信息，通过网络安全设备实施网络访问控制操作，修复被破坏的信息系统。网络攻击事件视情况采取 I、II 或 III 级响应。

5.6 有害程序事件：调取行为审计系统等相关网络设备数据，判断病毒、木马、僵尸网络的影响范围和严重程度；依据安全响应分级，结合具体情况，做出相应处理。

5.7 其他不确定安全事件：采取先关闭网络接口或停止信息发布服务，再进行问题分析、取证的原则。

6 后期处置及保障

6.1 后期处置

发生网络与信息安全事件，限期处置后，事件涉及业务部门需填写《网络安全事件（风险）处理单》（附件 1），网络信息中心根据整改情况恢复相应服务。

发生网络与信息安全事件，规定期限内无法处置的，仍需对外提供服务的，事件涉及业务部门需填写《网络安全事件（风险）处理单》，并另行签订网络安全责任书（附件 2），由学校网络安全与信息化工作领导小组组长签字后，网络信息中心根据具体情况暂时恢复相应服务。

学校表彰奖励在网络与信息安全处置工作中作出突出贡献的单位和个人，追究引起重大舆情和造成重大负面影响、不良后果的相关责任人的责任。

6.2 应急保障

6.2.1 信息保障。建立健全并落实网络与信息安全突发事件信息的收集、传递、报送、处理等各环节运行机制，完善信息传输渠道，确保信息报送渠道的安全畅通。

6.2.2 资金保障。网络信息中心应根据校园网络与信息系统安全预防和应急处置工作的实际需要，申报网络与信息系统关键设备及软件的运维专项资金，提出本年度应急处置工作的相关经费，上报计划财务处纳入年度预算，由学校给予资金保障。将应急资金纳入财务预算，为突发事件舆情处置工作提供必要的财力支持。

6.2.3 队伍保障。加强队伍建设，不断提高安全岗位工作人员的信息安全防范意识和技术水平，确保安全事件处置得当。其他部门、单位相关人员作为网络与信息安全突发事件应急预备队，可根据工作需要，安排应急工作。

6.2.4 安全培训和演练。网络信息中心不定期对相关工作人员进行网络与信息系统安全知识培训，增强预防意识和应急处置能力，有针对性地开展应急演练，确保相关措施有效落实。

7 附则

7.1 本预案由网络安全与信息化工作领导小组办公室负责解释。

7.2 本预案自印发之日起实施。

附件：1.山东理工大学网络安全事件（风险）处理单

2.山东理工大学网络安全责任书

附件 1

山东理工大学网络安全事件（风险）处理单

<table>
<tr><td rowspan="7">情况说明</td><td>单位名称</td><td colspan="4"></td></tr>
<tr><td>网站或信息系统名称</td><td colspan="2"></td><td>域名/IP</td><td></td></tr>
<tr><td>受理人员</td><td colspan="2"></td><td>受理时间</td><td></td></tr>
<tr><td rowspan="4">安全情况</td><td>级　　别</td><td colspan="2">☐IV 级　☐III 级　☐II 级　☐I 级</td><td rowspan="2">描述：详细情况见附页</td></tr>
<tr><td>紧急程度</td><td colspan="2">☐紧急 ☐一般</td></tr>
<tr><td>处理建议</td><td colspan="3">☐修复系统漏洞　☐修复程序漏洞　☐增加密码强度
☐其他</td></tr>
<tr><td>处置期限</td><td colspan="3"></td></tr>
<tr><td rowspan="8">单位处理信息(单位填写)</td><td>单位负责人</td><td colspan="2"></td><td>单位电话</td><td></td></tr>
<tr><td rowspan="2">系统管理员</td><td>姓名</td><td></td><td>E-mail</td><td></td></tr>
<tr><td>电话</td><td></td><td>手机</td><td></td></tr>
<tr><td>处理方式</td><td colspan="4">☐修复系统漏洞　☐修复程序漏洞 ☐增加密码强度
☐其他_____</td></tr>
<tr><td>处理细节</td><td colspan="4">(含修复时间)可附页</td></tr>
<tr><td>处理结果</td><td colspan="4">☐已处理　　☐忽略安全风险　　☐其他_____</td></tr>
<tr><td>说明</td><td colspan="4">1.在应用系统遭遇攻击、暴露漏洞之时，网络信息中心会根据风险级别和紧急程度对系统进行关停或者禁止访问等安全措施，以保证数据安全、并防止影响扩散。
2.完成处置后，填写本单，并完成相关签字、盖章流程，提交纸质文档到网络信息中心。
3.网络信息中心收到此单后，协助恢复单位的应用系统或者网站的正常服务。
4.事件处置期限内，无法按时处理的，仍需对外提供服务的，请另行签订网络安全责任书。</td></tr>
<tr><td>上线申请</td><td colspan="4">☐申请上线　　☐申请临时上线_____至_____</td></tr>
<tr><td colspan="5">我单位已阅读上述说明，并已完成处置，并愿意承担系统上线运行的相关后果。
单位负责人签字：
单位盖章：　　年　月　日</td></tr>
<tr><td rowspan="4">修复检查(网络信息中心填写)</td><td rowspan="3">修复检测</td><td>检测人</td><td></td><td>检测时间</td><td></td></tr>
<tr><td>检测结果</td><td colspan="3">☐已修复　☐未修复　☐其他
_____</td></tr>
<tr><td>处理意见</td><td colspan="3">☐同意上线　☐暂缓上线　☐临时上线_____至
_____</td></tr>
<tr><td colspan="3">检测人签字：
年　月　日</td><td colspan="2">网络信息中心领导签字：
年　月　日</td></tr>
</table>

附件 2

山东理工大学网络安全责任书

本信息系统（域名：　　IP:　　）在从事信息服务过程中，因发生网络与信息安全事件，规定期限内无法按时处置，仍需提供服务，郑重承诺遵守本责任书所列事项，对所列事项负责。如有违反，由本部门（单位）承担由此带来的相应责任。

一、遵守《山东理工大学网络安全管理规定》相关规定，按照“谁主管谁负责，谁运营谁负责，谁使用谁负责”的原则，做好本信息系统的运维和管理工作。

二、用户在学校网站群和虚拟机上建立的网站，原则上只允许开通 80 端口用于外网网页的访问。用户在网站群上建立的信息系统，只需要负责系统内容的建设和管理，网络信息中心将负责系统软硬件的运行、维护和管理。用户在虚拟机上建立的信息系统，需要负责系统软件、应用软件和系统内容的建设、维护和管理，网络信息中心负责系统硬件平台的维护和管理。

用户申请设立具有独立服务器的信息系统（放置在学校托管机房或自我保管），原则上只允许开通 80 端口用于外网网页的访问，用户负责该信息系统所有软硬件系统的建设、维护和管理，网络信息中心提供网络接入和域名解析服务。

三、用户应建立信息安全责任制度，落实信息系统管理员、日常运维人员，做好信息安全事故应急处置预案，严格审核网站发布内容，合理分配信息发布权限，保证信息发布内容的合法和安全。

四、确定专人做好信息系统的日常维护和管理工作，记录和保存访问日志，及时跟踪运行状况，及时对信息系统进行安全升

级和技术维护，出现异常情况应按应急处置预案处置并向网络信息中心报告。信息系统管理人员有义务按照网络信息中心的要求报告系统的使用情况、运行情况和维护情况等，并接受相关检查。

五、网络信息中心定期对信息系统进行安全扫描和检测，对发现安全隐患的，将立即通过邮件或短信等方式通知管理人员要求限时整改并关闭外网访问，管理人员有义务在规定时间内按照网络信息中心的要求做好信息系统的安全整改工作。在信息系统出现重大网络信息安全问题时，网络信息中心可在未事先告知的情况下，断开信息系统与校园网的连接，停止相关服务。

六、责任书各条款不因负责人变化而变更或解除，接任负责人应履行相应职责。

本责任书一式两份，网络安全与信息化工作领导小组办公室和责任部门（单位）各执一份。

本责任书自签署之日起生效，由网络安全与信息化工作领导小组负责解释。

网络安全与信息化工作领导小组　　责任单位（章）

负责人（签字）　　单位负责人（签字）

年　月　日　　年　月　日

抄送：各党总支（党委），校党委各部门、各群团组织。

山东理工大学校长办公室　　2019 年 7 月 1 日印发